UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/038,365	01/03/2002	Genevieve Bell	42390P13661	6983

8791 7590 09/14/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
LAM, HUNG H	
ART UNIT	PAPER NUMBER
2615	

DATE MAILED: 09/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/038,365	**Applicant(s)** BELL ET AL.	
	Examiner Hung H. Lam	**Art Unit** 2615	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9,19,23,24,26-29,31,33-35,37-39 and 41-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9,19,23-24,26-29,31,33-35,37-39 and 41-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The amendments, filed on 06/13/05, have been entered and made of record. Claims 36, 40 and 44 have been cancelled. Claims 9, 19, 23-24, 26-29 31, 33-35, 37-39 and 41-43 are pending.

2. The affidavit filed on 06/13/05 under 37 CFR 1.131 is sufficient to overcome the Gennetten reference.

Response to Arguments

3. Applicant's arguments with respect to claims 9, 19, 23, 24, 26, 27, 28, 29, 31, 33, 34, 35, 37, 38, 39, 41, 42, 43 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 9, 19, 23, 24, 26, 27, 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Friedman (US-5,499,294) in view of Parulski (US- 6,567,119) and further in view of Steinberg (US-6,433,818).

Regarding **claim 9**, Friedman describes a digital photography subsystem comprising:

a decryption module (Friedman: figure 3c, item 20) to accept image data and metadata from a digital camera, the metadata including a digital signature of the image data, to verify the digital signature of the image data, and to examine the metadata to determine authenticity of the image data (Friedman: column 6, lines 2-7), and a viewer module (or display) to display the image data when the decryption module indicates the image data is authentic (Friedman: figure 4), wherein the metadata comprises a geographic location (through the global positioning system (GPSI) of the digital camera when the image was captured (Friedman: column 4, line 60) and at least one of: date and time the image was captured (Friedman, column 4, Lines 59), identifier of the camera owner, identifier of the photographer, and focal distance (Friedman: column 4, Lines 61), white levels (Friedman: column 4, Lines 59), f-stop (Friedman: column 4, Lines 59), brightness compensation (column 4, Lines 59), and distance for auto-focus when the image was captured (column 4, Lines 61-63).

Friedman further describes the use of a public key, taken from the image border or nameplate, as a serial number for identifying the camera for such purposes as - warranty repair or replacement. The public key is in fact mathematically related to the camera's private key (column 6, Lines 14-21). So, the public key can be used as a means of identifying either the owner or the photographer of the camera since every camera and its owner has its own unique means of identifying itself from any other camera.

However, Friedman does not teach a digital photography subsystem wherein the image data and metadata is associated with audit data indicating changes made to the image data since capture, and the viewer module is configured to display the audit data and the metadata. Parulski describes an editing step 82 (Parulski; Fig. 4) where the metadata lists this editing data in the advanced edits list 100 (or audit data) to describe edits performed by an applications program other than modifying the standard FlashPix viewing parameters (Parulski; Col. 6, Ln. 15-32). In addition, the metadata may also include a copy of the unmodified thumbnail image in the thumbnail image data 98, which can be compared to the modified thumbnail image data 23 to determine if any changes have been made to the original image data by subsequent image editing applications (Parulski: column 6, lines 23-32 and figure 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the digital photography subsystem of Friedman to include image data and metadata associated with audit data indicating changes made to the image data since capture. One would have been motivated to modify the digital photography subsystem of Friedman to include image data and metadata associated with audit data indicating changes made to the image data because Parulski teaches that if an "older" printer does not recognize the modifications made in the extension data, then the original image data could then be used (Parulski: column 6, lines 1 1-25).

However, Friedman in view of Parulski fails to disclose that a fingerprint data obtained from a fingerprint reading device on the digital camera at the time the image was captured, and the fingerprint data is used to identifying the operator of the digital camera.

In the same field of endeavor, Steinberg teaches a camera with biometric security wherein fingerprint/ biometric data obtaining from the shutter button (Fig. 10; 142) or any points of contact between finger and camera body is used for identifying and limiting access to an authorized user (Steinberg ; Col. 5, Ln. 35-45; Col. 6, Ln. 5-35). Steinberg further teaches that the fingerprint data is captured and compared with a signature data in order to grant or not grant camera access (Steinberg; Col. 7, Ln. 29- Col. 8, Ln. 1-40). Additionally, Steinberg teaches image data in encrypted form which is decrypted by only owner's key (Steinberg; Col. 5, Ln. 12-34). In light of the teaching from Steinberg, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Friedman and Parulski to obtain fingerprint data from any points of contact between camera body and finger as claimed by Steinberg in order to only grant access an authorized user and thereby providing a digital camera with theft protection and allowing only an authorized user to view the encrypted image (Steinberg; Col. 1; Ln. 58-67).

Regarding **claim 19**, Friedman describes a method of generating secure digital photographic data comprising:

capturing image data representing an image in the physical world by a digital camera (Friedman: column 3, Lines 64-66);

obtaining metadata associated with the captured image, the metadata comprising a geographic location of the digital camera when the image was captured, and at least one of: date and time the image was captured (Friedman: column 4, Lines 59), identifier of the camera owner, identifier of the photographer, and focal distance (Friedman: column, Lines 61), white levels (Friedman: column 4, lines 59), f-stop (Friedman: column 4, Lines 59), brightness compensation (Friedman: column 4, Lines 59), and distance for auto-focus when the image was captured (Friedman: column 4, Lines 61-63).

Friedman further describes the use of a public key, taken from the image border or nameplate, as a serial number for identifying the camera for such purposes as warranty repair or replacement. The public key is in fact mathematically related to the camera's private key (Friedman; column 6, Lines 14-21). So, the public key can be used as a means of identifying either the owner or the photographer of the camera since every camera and its owner has its own unique means of identifying itself from any other camera.

digitally signing the image data and the metadata with a private key of an asymmetric key pair (Friedman; column 5, lines 49-65; Friedman described an encryption module configured to digitally sign the image data prior to storage using a private key of an asymmetric key pair and to obtain metadata associated with the image data); and

storing the image data and metadata in a memory of the digital camera (Friedman; Col. 5, Ln. 65 - Col. 6, Ln. 1-11).

However, Friedman does not teach method of generating secure digital photographic data wherein the metadata includes audit data indicating changes made to the image data since capture. Parulski describes an editing step 82 (Fig. 4) where the metadata lists this editing data in the advanced edits list 100 (or audit data) to describe edits performed by an applications program other than modifying the standard FlashPix viewing parameters (Parulski; Col. 6, Ln. 15-32). In addition, the metadata may also include a copy of the unmodified thumbnail image in the thumbnail image data 98, which can be compared to the modified thumbnail image data 23 to determine if any changes have been made to the original image data by subsequent image editing applications (Parulski: column 6, lines 23-32 and figure 5). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of generating secure digital photographic data of Friedman to include image data and metadata associated with audit data indicating changes made to the image data since capture. One would have been motivated to modify the method of generating secure digital photographic data of Friedman to include image data and metadata associated with audit data indicating changes made to the image data because Parulski teaches that if an "older" printer does not recognize the modifications made in the extension data, then the original image data could then be used (Parulski: column 6, Lines 11-25).

However, Friedman in view of Parulski fails to disclose that a fingerprint data obtained from a fingerprint reading device on the digital camera at the time the image was captured, and the fingerprint data is used to identifying the operator of the digital camera.

In the same field of endeavor, Steinberg teaches a camera with biometric security wherein fingerprint/ biometric data obtaining from the shutter button (Fig. 10; 142) or any points of contact between finger and camera body is used for identifying and limiting access to an authorized user (Steinberg; Col. 5, Ln. 35-45; Col. 6, Ln. 5-35). Steinberg further teaches that the fingerprint data is captured and compared with a signature data in order to grant or not grant camera access (Steinberg; Col. 7, Ln. 29- Col. 8, Ln. 1-40). Additionally, Steinberg teaches image data in encrypted form which is decrypted only by owner's key (Steinberg; Col. 5, Ln. 12-34). In light of the teaching from Steinberg, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Friedman and Parulski to obtain fingerprint data from any points of contact between camera body and finger as claimed by Steinberg in order to only grant access an authorized user and thereby providing a digital camera with theft protection and allowing only an authorized user to view the encrypted image (Steinberg; Col. 1; Ln. 58-67).

Regarding **claim 23**, Friedman in view of Parulski and further in view of Steinberg further discloses the method of claim 19 wherein the private key is uniquely associated with the digital Camera (Friedman, abstract; Col. 5, Ln. 49-60).

Regarding **claim 24**, Friedman in view of Parulski and further in view of Steinberg further describes the method of claim 19 wherein the private key is uniquely associated with the manufacturer of the digital camera (Friedman, column 4, Lines 38-40).

Regarding **claim 26**, Friedman teaches a method of generating and authenticating digital photographs comprising:

capturing image data representing an image in the physical world by a digital camera (Friedman: column 3, Lines 64-66);

obtaining metadata associated with the captured image, the metadata indicating characteristics of the image data (Friedman: column 4, lines 55-66);

determining a geographic location of the digital camera when capturing the image and wherein the metadata comprises the geographic location of the camera when the image was captured (Friedman: column 4, Lines 66-67 and column 5, lines 1-4);

digitally signing the image data and the metadata with a private key of an asymmetric key pair (Friedman: column 5, Lines 49-65); and

transferring the image data, the digital signature, and the metadata to a host system (Friedman: column 1, Lines 4-45);

authenticating the image data by the host system using the digital signature, a corresponding public key of the asymmetric keys pair, and the metadata (Friedman: column 6, lines 2-15).

However, Friedman does not teach a method of generating and authenticating digital photographs comprising wherein updating audit data describing changes made to the image data, and associating the audit data with the image data and the metadata. Parulski describes an editing step 82 (Parulski; Fig. 4) where the metadata lists this editing data in the advanced edits list 100 (or audit data) to describe edits preformed by an applications program other than modifying the standard FlashPix viewing parameters (Parulski; Col. 6, Ln. 15-32). In addition, the metadata may also include copy of the unmodified thumbnail image in the thumbnail image data 98, which can be compared to the modified thumbnail image data 23 to determine if any changes have been made to the original image data by subsequent image editing applications (Parulski: column 6, Lines 23-32 and figure 5). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of generating and authenticating digital photographs of Friedman to include image data and metadata associated with audit data indicating changes made to the image data since capture. One would have been motivated to modify the method of generating and authenticating digital photographs of Friedman to include image data and metadata associated with audit data indicating changes made to the image data because Parulski teaches that if an "older' printer does not recognize the modifications made in the extension data, then the original image data could then be used (Parulski: column 6, Lines 11-25).

However, Friedman in view of Parulski fails to disclose a fingerprint data obtained from a fingerprint reading device on the digital camera at the time the image was captured, and the fingerprint data identifying the operator of the digital camera.

In the same field of endeavor, Steinberg teaches a camera with biometric security wherein fingerprint/ biometric data obtaining from the shutter button (Steinberg; Fig. 10; 142) or any points of contact between finger and camera body is used for identifying and limiting access to an authorized user (Steinberg; Col. 5, Ln. 35-45; Col. 6, Ln. 5-35). Steinberg further teaches that the fingerprint data is captured and compared with a signature data in order to grant or not grant camera access (Steinberg; Col. 7, Ln. 29- Col. 8, Ln. 1-40). Additionally, Steinberg teaches image data in encrypted form which is decrypted only by owner's key (Steinberg; Col. 5, Ln. 12-34). In light of the teaching from Steinberg, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Friedman and Parulski to obtain fingerprint data from any points of contact between camera body and finger as claimed by Steinberg in order to only grant access an authorized user and thereby providing a digital camera with theft protection and allowing only an authorized user to view the encrypted image (Steinberg; Col. 1; Ln. 58-67).

With respect to the limitation the metadata including the fingerprint data,

Friedman as modified by Parulski teaches a method of associating image data and metadata with audit data for authenticating digital photographs (Parulski: column 6, Lines 11-25). Steinberg teaches that the fingerprint data is captured and compared with a signature data in order to grant or not grant camera access (Steinberg; Col. 7, Ln. 29- Col. 8, Ln. 1-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Friedman and Parulski to include the captured fingerprint data of Steinberg in the metadata in order to provide an encrypted image wherein only the owner of the fingerprint data is authorized to view the encrypted image.

Regarding **claim 27**, Friedman in view of Parulski and further in view of Steinberg further describes the (currently amended) method of claim 26, wherein the metadata comprises at least one of: date ant time the image was captured by the digital camera (Friedman: column 4, Lines 59), identifier of the camera owner, identifier of the camera owner, and Friedman further describes the use of a public key, taken from the image border or nameplate, as a serial number for identifying the camera for such purposes as warranty repair or replacement. The public key is in fact mathematically related to the camera's private key (Friedman; column 6, Lines 14-21). So, the public key can be used as a means of identifying either the owner or the photographer of the camera since every camera and its owner has its own unique means of identifying itself from any other camera; focal distance (Friedman: column 4, Lines 61), white levels (Friedman: column 4, Lines 59), f-stop (Friedman: column 4, Lines 59), brightness compensation

(Friedman: column 4, line 59), and distance for auto-focus when the image was captured (Friedman: column 4, lines 61-63).

Regarding **claim 31**, Friedman in view of Parulski and Steinberg further describes the method of claim 26 further comprising displaying the image data when authenticated (Friedman; Fig. 4; column 4, Lines 47-57).

6. Claim 28 is rejected under 35 U.S.C. 103(c) as being unpatentable over U.S. Friedman in view Parulski, in view of Steinberg and further in view of Davis (US-2002/0,001,395).

Regarding **claim 28**, Friedman in view of Parulski and further in view of Steinberg describes the method of claim 27, but does not teach the method further comprising obtaining the date and time setting for the digital camera by a host system from a website controlled by at least one of the manufacturer and the distributor of the digital camera.

In the same field of endeavor, Davis teaches a session mode wherein the camera operates under the control of parameters that govern that session (Davis; [0066], lines 2-4). In addition, Davis teaches that an external device may initiate that session (Davis; [0066], lines 6-8). An external device may in fact be a communications network, such as the internet (Davis; figure 2, item 102). Davis also teaches that within the session parameters, the external device can instruct the camera to set the time and date (Davis; [0067], lines 3-6). Also, note that Davis teaches that the either the user can initiate a session or and external device can (Davis; [0066], Lines 6-8). A non-user external device that initiates instructions to the camera could in fact comprise either the distributor or the manufacturer, as they are not the camera user. Therefore, it would have been obvious to one familiar to the art to combine the method taught in Friedman, Parulski and Steinberg with a website controlled from either the distributor or manufacturer to set the camera's time and date. One would have been motivated to modify Friedman, Parulski and Steinberg to include a website controlled by either the manufacturer or the distributor to keep the photographer from altering the photographing record in that it would be false and misleading as stated in Davis (Davis; [0065]).

7. Claim 29 is rejected under 35 U.S.C. 103(c) as being unpatentable over Friedman in view of Parulski, in view of Steinberg further in view of Steinberg'949 (US-6,587,949)

Regarding **claim 29**, Friedman in view of Parulski and further in view of Steinberg fails to disclose the method comprising updating the private key for the digital camera by the host system from a website controlled by at least one of the manufacturer and the distributor of the digital camera.

In the same field of endeavor, Steinberg'949 teaches the initial programming of a security key, or private key, which is done with the initial set-up of the device, prior to its normal use (Steinberg'949; column 6, lines 45-58). Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the method taught in Friedman, Parulski and Steinberg with the programming of a private key prior to using the device.

One would have been motivated to modify the method of Friedman, Parulski and Steinberg to include the programming (updating) of a private key in that with the user knowing the private key, they can then operate the computer to decrypt the encrypted data as stated in Steinberg'949 (Steinberg'949; column 6, lines 58-60).

8. Claims 33-35, 37-38, 39 and 41-43 are rejected under 35 U.S.C. 103(c) as being unpatentable over Friedman in view of Parulski, in view of Steinberg and further in view of Tsukamoto (US-6,359,837).

Regarding **claims 33, 37, and 41**, Friedman in view of Parulski and further in view of Steinberg fails to disclose the method wherein the metadata further comprises a temperature reading obtained from thermometer on the digital camera at the time the image was captured.

In the same field of endeavor, Tsukamoto teaches a method of obtaining weather information wherein temperature from a sensor is transferred to and recorded by the image recording apparatus together with an image (Tsukamoto: column 15, lines 20-39 and figure 14). Therefore it would have been obvious to one familiar to the art to combine the subsystem or method taught in Friedman in view of Parulski and Steinberg to include a temperature reading obtained from thermometer on the digital camera at the time the image was captured. One would have been motivated to modify the subsystem or method of Friedman, Parulski and Steinberg to include a temperature reading obtained from thermometer on the digital camera at the time the image was captured of Tsukamoto in that the user can carry the wristwatch and digital camera combination on a trip or mountain climbing and electronically record various situations (Tsukamoto: column 1, lines 29-44).

Regarding **claims 34, 38, and 42**, Friedman in view of Parulski and further in view of Steinberg fails to teach a digital photography subsystem wherein the metadata further comprises a barometer reading obtained from the barometer on the digital camera at the time the image was captured. However, the limitations are well known in the art as taught by Tsukamoto.

In the same field of endeavor, Tsukamoto teaches the use of an atmospheric pressure sensor (barometer) (Tsukamoto: column 1, Lines 29-38) that is transferred to and recorded by the image recording apparatus together with an image (Tsukamoto: column 15, Lines 20-39 and figure 14). In light of the teaching from Tsukamoto, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Friedman, Parulski and Steinberg by having a barometer reading from the barometer / atmospheric pressure sensor on the digital camera of Tsukamoto in order to record the atmospheric level along with the captured image (Tsukamoto: column 15, Lines 20-39 and figure 14).

Regarding **claims 35, 39 and 43**, Friedman in view of Parulski and further in view of Steinberg further fails to disclose the method, wherein the metadata comprises a compass reading obtained from a compass on the digital camera at the time the image was captured. However, the limitations are well known in the art as taught by Tsukamoto.

In the same field of endeavor, Tsukamoto teaches the use of a compass that is transferred to and recorded by the image recording apparatus together with an image (Tsukamoto: column 15, lines 20-39 and figure 14). In light of the teaching from Tsukamoto, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Friedman, Parulski and Steinberg by having a compass reading from the compass on the digital camera of Tsukamoto in order to record the atmospheric level along with the captured image (Tsukamoto: column 15, Lines 20-39 and figure 14).

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hung H. Lam whose telephone number is 571-272-7367. The examiner can normally be reached on Monday - Friday 8AM - 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Ometz can be reached on 571-272-7593. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HL

08/30/05

NGOC-YEN VU
PRIMARY EXAMINER